

Abstract of the Invention

A single-photon “watch dog” detector for a two-way quantum key distribution (QKD) system. The detector can detect weak probe signals associated with a Trojan horse attack, or weak substitute signals associated with a “man in the middle” attacks. The detector provides for a significant increase in security for a two-way QKD system over the prior art that employs a conventional detector such as a photodiode. By counting the number of weak pulses entering and/or leaving the reflecting QKD station (Alice), an eavesdropper that attempts to add weak pulses to the quantum channel in order to gain phase information from the phase modulator at Alice can be detected.